Diplom-Mathematiker Jens Fankhänel

Ein rechtssicheres elektronisches Verfahren zur Bestätigung der Paketannahme

1. Auflage, Stand: 16. April 2024

Diplom-Mathematiker Jens Fankhänel
Ein rechtssicheres elektronisches Verfahren zur Bestätigung der Paketannahme
1. Auflage, Stand: 16. April 2024

Inhaltsverzeichnis

1 Einleitung **4**

2 Erläuterung des Prinzips **5**

3 Die Details **6**
3.1 Speicherung der öffentlichen Schlüssel 6
3.2 Beschleunigung der Paket-Auslieferung 6

4 Von der Paketnummer zur Dokumentnummer **7**

Literaturverzeichnis 8

A Tipps zum Papiersparen **9**
A.1 Kataloge 9
A.2 Zeitungen und Zeitschriften 9
A.3 Telefonbücher 9

1 Einleitung

Paketdienste in der BRD lassen sich die Auslieferung ihrer Pakete nur noch per Unterschrift auf einem Tablet-Computer bestätigen. Jedoch ist dieses Verfahren nach unserer Überzeugung nicht rechtssicher.
Trotzdem hat das sehr unsichere Verfahren sich leider immer weiter ausgebreitet. Auch Speditionen lassen sich die Anlieferung ihrer Fracht durch die Unterschrift auf einem Tablet-Computer bestätigen. Sogar in der öffentlichen Verwaltung ist es nach unserer Erfahrung schon vorgekommen, dass einem Bürger ein Dokument zur Unterzeichnung auf einem Tablet-Computer vorgelegt wurde.
Um Verträge wieder sicherer zu machen, stellt der Autor hier ein alternatives elektronisches Verfahren zum Signieren vor. Eine herkömmliche Unterschrift, die aus dem handgeschriebenen Namen besteht, soll nie auf ein elektronisches Gerät gezeichnet werden. In diesem Artikel wird gezeigt, dass ein Zahlencode genügt, um zu beweisen, dass ein bestimmter Bürger ein bestimmtes Dokument unterzeichnet hat. Allein durch die Eingabe eines Zahlencodes ist die elektronische Signatur vollständig.
Herkömmliche Unterschriften gehören immer nur auf einen Bogen Papier! Das sollten die Behörden und die Unternehmen sich dick einrahmen.

2 Erläuterung des Prinzips

Jeder Paketkunde erzeugt mit dem bekannten RSA-Verfahren[1] ein Schlüsselpaar. Der öffentliche Schlüssel des Kunden wird auf einem Server hinterlegt. Den privaten Schlüssel kennt allein der Kunde.
Der Kunde verschlüsselt die Paketnummer mit seinem privaten Schlüssel und bekommt dadurch den Zahlencode, den er zur Bestätigung der Paketannahme braucht. Jeder Mensch, der diesen Bestätigungs-Code kennt, kann ihn mit Hilfe des öffentlichen hinterlegten Schlüssels des Kunden entschlüsseln. Wenn durch die Entschlüsselung wieder die Paketnummer erzeugt wird, dann war der Bestätigungs-Code korrekt.
Insbesondere wird Folgendes bewiesen: Wer den Bestätigungs-Code zur Paketnummer kannte, muss den privaten Schlüssel, der zum öffentlichen Schlüssel des Kunden gehört, besitzen. Das ist im Allgemeinen nur der Kunde selbst, sofern er seinen privaten Schlüssel nicht weitergegeben hat und ihm der private Schlüssel nicht gestohlen wurde. Damit ist gesichert, dass der Kunde unterzeichnet hat. Das Verfahren ist für den Paketdienst sogar noch sicherer als eine herkömmliche Unterschrift, die mitunter auch gefälscht werden kann.

3 Die Details

3.1 Speicherung der öffentlichen Schlüssel

Die öffentlichen Schlüssel aller Paket-Kunden und Paket-Kundinnen müssen auf dem Server einer unabhängigen Organisation gespeichert werden. Es wäre zwar durchaus sicher, den öffentlichen Schlüssel auf der Homepage des Kunden zu hinterlegen. Aber nicht jeder Paket-Kunde besitzt eine eigene Homepage. Darum sollten die öffentlichen Schlüssel aller Paket-Kunden und Paket-Kundinnen von einer unabhängigen Organisation verwaltet werden.
Ein Kunde sollte sein Schlüsselpaar ändern können, wenn er es nicht mehr für sicher hält. In diesem Fall sollte der Server alle bisherigen öffentlichen Schlüssel des Kunden mit dem jeweiligen Zeitraum ihrer Gültigkeit speichern. Dann kann bestätigt werden, dass ein Paket angenommen wurde, als noch ein anderes Schlüsselpaar galt.

3.2 Beschleunigung der Paket-Auslieferung

Verwendet der Kunde einen privaten Schlüssel mit mehr als 2.000 Dezimalstellen, dann ist die RSA-Verschlüsselung nach heutigen Standards sehr sicher. Aber die Verschlüsselung erzeugt einen Bestätigungs-Code, der selbst mehr als 2.000 Dezimalstellen lang ist. Würde jeder Kunde mehr als 2.000 Ziffern per Hand eingeben, dann könnten erhebliche Verzögerungen bei der Paket-Auslieferung auftreten.
Um die Paket-Auslieferung zu beschleunigen, sollte der Kunde seinen Bestätigungs-Code auf einem USB-Stick abspeichern. Vor jeder Annahme eines Pakets ist eine kurze Sitzung am heimischen Computer notwendig, um einen oder mehrere Bestätigungs-Codes auf dem Stick zu speichern.
Wenn der Paketbote kommt, steckt der Kunde seinen Stick an einen tragbaren Computer des Paketdienstes. Der Computer liest die abgespeicherten Bestätigungs-Codes.
Als Alternative zum USB-Stick könnte man auch eine wiederbeschreibbare Chipkarte verwenden. Die Signatur mit einer Chipkarte würde sich wie die Bezahlung mit einer Geld- oder Kreditkarte anfühlen. Andererseits sind Schreibgeräte für Chipkarten bisher kaum verbreitet.

4 Von der Paketnummer zur Dokumentnummer

Bisher wurde das Verfahren zum sicheren Signieren nur für die Pakete eines einzigen Paketdienstes erklärt. Jedoch kann das Verfahren für das Signieren aller möglichen Dokumente verwendet werden. Darum ist es ratsam, das Verfahren gleich zukunftssicher für das Signieren sehr unterschiedlicher Dokumente zu machen.
Mit 50-stelligen Zahlen können alle Dokumente, die in den nächsten 500 Jahren auf der ganzen Welt unterzeichnet werden sollen, eindeutig identifiziert werden. Die Paketnummer sollte ganz hinten in der 50-stelligen Dokumentnummer stehen. Ganz vorn in der Dokumentnummer sollte ein Ländercode stehen. Außerdem kann noch einen Branchen-Code und eine Nummer für jeden Paketdienst in der Dokumentnummer enthalten sein. Stellen, die vorläufig noch nicht benötigt werden, füllt man einfach mit Nullen.
Anstelle der Paketnummer sollte also die 50-stellige Dokumentnummer verschlüsselt werden. Nach der Entschlüsselung erhält man wieder die 50-stellige Dokumentnummer, die auch die Paketnummer enthält. Ansonsten bleibt das Verfahren so, wie es in den Kapitel 2 und 3 erklärt wurde.

Literaturverzeichnis

[1] R.L. Rivest, A. Shamir, and L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; URL: http://people.csail.mit.edu/rivest/Rsapaper.pdf

A Tipps zum Papiersparen

Anscheinend wollte jemand Papier sparen, als die Paketdienste anfingen, sich die Auslieferung ihrer Pakete durch die Unterschrift auf einem Tablet-Computer bestätigen zu lassen. Man kann jedoch noch viel mehr Papier sparen.

A.1 Kataloge

Gedruckte Waren-Kataloge werden nicht mehr gebraucht. Denn fast alle Kunden und Kundinnen der Industrie-Länder bestellen lieber im Internet als per Telefon. Besucht man die Webseite eines Händlers, dann kann man sehr bequem nachschauen, welche Waren gerade verfügbar sind. Im Internet bekommt man zu den Waren viele zusätzliche Informationen, die nicht alle in Katalogen abgedruckt werden können.

A.2 Zeitungen und Zeitschriften

Zeitungen und Zeitschriften müssen in den Industrie-Ländern nicht mehr gedruckt werden, weil man sie im Internet lesen kann. Kreuzwort-Rätsel kann man sich ausdrucken, was viel weniger Papier als der Druck einer ganzen Zeitschrift verbrauchen würde. Oder man könnte Kreuzwort-Rätsel interaktiv (zum Ausfüllen am Computer) gestalten. Dazu müssten die Zeitschriften eventuell ein paar Programmierer einstellen, was Arbeitsplätze schaffen würde.

A.3 Telefonbücher

Telefonbücher müssen in den Industrie-Ländern nur noch in einer sehr geringen Auflage für alte und behinderte Menschen sowie für Leute, die keinen Internet-Anschluss haben, gedruckt werden. Fast alle Menschen, die in hoch-entwickelten Ländern wohnen, suchen sich die benötigten Telefonnummern aus dem Internet.